Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An X.509 certificate stored on computer readable medium, said certificate capable of supporting more than one cryptographic algorithm, comprising:

a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

2. (Previously Presented) An X.509 certificate according to Claim 1, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

3. (Previously Presented) An X.509 certificate according to Claim 1, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

4. (Previously Presented) A method for enabling an X.509 certificate to support more than one cryptographic algorithm, said method comprising the steps of:

providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

5. (Previously Presented) A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

6. (Previously Presented) A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

7. (Presently Amended) Computer readable code stored on computer readable media for enabling an X.509 certificate to support more than one cryptographic algorithm, said computer readable code comprising:

first subprocesses for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

second subprocesses for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

third subprocesses for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

C3

8. (Previously Presented) Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

9. (Previously Presented) Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

10. (Newly Presented) In a computing environment, a system for enabling an X.509 certificate to support more than one cryptographic algorithm, said system comprising:

means for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

C4

means for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

means for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

11. (Newly Presented) A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

12. (Newly Presented) A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.